MSH Biswas Crypto-Intensive Technique

Md. Shamim Hossain Biswas*

* Department of Software Engineering, Daffodil International University
Bangladesh

DOI: 10.14299/ijser.2019.10.01
https://doi.org/10.14299/ijser.2019.10.01

Abstract—This research paper aims to attach a signature scheme that enables signature generation and signature verification to a well-defined cryptosystem. This is a combination of key generation, encryption, signature generation, signature verification, and decryption algorithms. The Michael O. Rabin signature scheme uses random padding to validate signatures. Similarly, the proposed cryptographic technique uses the same padding system with additional quadratic residue and floor value of quadratic quotient. The only difference is that Michael O. Robin's signature can be double or triple in some special cases, but the proposed model uses a four-tuple signature system. One ambiguity of the Michael O. Rabin cryptosystem is that it can generate the same ciphertext from different plaintexts and multiple plaintexts from a single ciphertext. To solve this issue, I constructed a cryptosystem proposing a mathematical solution, namely *"A mathematical model for ascertaining the same ciphertext generated from distinct plaintext in the Michael O. Rabin cryptosystem."* But that model did not have an authentication mechanism to verify the authenticity of the sender and the message. Because it had no signature scheme. The proposed crypto-intensive technique uses a two-time security key by slightly altering the Diffie-Hellman key exchange protocol. The proposed cryptographic method gives the sender an advantage in creating a signature using the encrypted text. On the other hand, the intended recipient can recover the original plaintext through a signature verification mechanism. The initial research initiative was to review different cryptosystem construction techniques and signature schemes, then apply those mathematical concepts to construct an effective cryptographic technique. This research starts with an exploratory research approach and ends with a computational research method. Data collection methods included a literature review, critical thinking strategies, solving various computational math problems, and focus group discussions. The people involved in my research were university professors. This research revealed an effective crypto-intensive technique that is secure against man-in-the-middle attacks. It is unforgeable, while Rabin's signature is forgeable in a forgery attack.

Index Terms—Cryptography, cryptosystem, Diffie-Hellman key-exchange protocol, Signature scheme, Bezout's Coefficient, Euclidean algorithm, Chinese Remainder theorem, Plaintext attack, Forgery attack. Man-in-the-middle attack, Digital Signature.

1 Introduction

The Rabin signature algorithm is a method of digital signature. It was one of the first digital signature schemes that related to the hardness of forgery. It is directly connected to the problem of integer factorization. In the random oracle model, it was existensitally unforgeable, assuming the integer factorization problem was intractable and closely related to the Rabin crptosystem [1]. Since its publication, a large amount of research was carried out by several researchers on Michael O. Rabin signature scheme [2].

A digital signature is a mathematical technique for verifying the authenticity of digital messages or documents. Authentication means that a valid digital signature gives a recipient very strong reason to believe that the message was created by a known sender, and integrity ensures that the message was not altered in transit. It is a standard element of most cryptographic protocols and is commonly used for software distribution, financial transactions, contract management systems, and to detect forgery or tampering, especially in the intentional modification of products. The term tempering refers to many forms of sabotage. The term authentification can refer to a computer communication protocol. A cryptographic protocol is specifically designed for the transfer of authentication data between two entities. Data integrity actually refers to the maintenance and the assurance of the accuracy and consistency of data over its entire life-cycle.

Digital signatures employ asymmetric cryptography. In many instances, they provide a layer of validation and security to messages sent through a non-secure channel. Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals, but properly implemented digital signatures are more difficult to forge than the handwritten type. It can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message while also claiming their private key remains secret. Further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages can be anything representable as a bitstring: Examples include a message sent via electronic mail, contracts, or some other cryptographic protocol. It typically consists of three algorithms:

1. *The key generation algorithm* randomly selects a private key from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
2. *The signing algorithm* produces a digital signature.
3. *The signature-verification algorithm* claims about the message's authenticity.

Two main properties are required for digital signature: in the beginning, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. In addition to that, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the generator of the message to attach a code that acts as a signature.

The Rabin cryptosystem can also be used to create a signature by exploiting the inverse mapping. To sign a message(m), the signer must solve an equation $x^2 = m \ mod \ N$ and any of the four roots(S) can be used to form the signed message (m, S). However, if $x^2 = m \ mod \ N$ has no solution, signature cannot be constructed directly. To overcome this issue, a random pad U is used until $x^2 =$ m $*$ U mod N is solvable. And then the signature will be triple (m, U, s). The verifier compares s^2 with m $*$ U mod N and accepts the signature as valid when these two numbers are equal.

The encryption mechanism uses quadratic residue to produce cipher text. The encryption of a message $m \in z*_N$ is presented by $c = m^2 \ mod \ N$, where $N = p * q$ is a product of two prime numbers, and decryption is performed by solving the equation $x^2 = c \ mod \ N$, N which has four roots. Thus, for complete decryption, further information is needed to identify message(m) among the roots. It has a vulnerabilityy to chosen-plaintext attacksk [3–6]. There is a timing attack on the modularr exponentiation algorithm [7]. The observer actually observes the exponentiation time of the algorithm. An attacker can reveal information about a message because the execution time depends on the number ones in the binary representation of the message.

The decryption was accomplished by computing two square roots, Bezout's coefficient using an extended Euclidean algorithm and combining them with the Chinese-remainder-theorem. Similarly to the RSA and ElGamal cryptosystems, the Michael O. Rabin cryptosystem is described in a ring under addition and multiplication modulo composite integers. One of the main disadvantages is that it generates four results during decryption, and extra effort is needed to sort out the right one out of the four possibilities. Michael O. Rabin's signature is vulnerable to a forgery attack.

The proposed cryptographic method is able to encrypt and decrypt messages using a standard symmetric key algorithm called the Diffie-Hellman key exchange protocol [8]. The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography. It is vulnerable to a "man-in-the-middle attack." A number of commercial products employ this key exchange technique. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption and decryption of messages. The algorithm itself is limited to the exchange of secret values. The Diffie-Hellman algorithm's effectiveness depends on computing discrete logarithms. The algorithm has a number of steps:

Global public elements: N is a prime number that can define a domain, so-called curve area, or elliptic curve, α is a primitive root of N such that α < N.

Key generation for user A: Select private key X_a such that $X_a < N$. Calculate the public *key* $Y_a = \alpha^{xa} \ mod \ N$.

Key generation for user B: Select a private key X_b such that $X_b < N$ and calculate the public key $Y_b = \alpha^{xb} \ mod \ N$.

Secret key for user A: $K = (Y_b)^{xa} \ mod \ N$.
Secret key for user B: $K = (Y_a)^{xb} mod \ N$.

Let's consider a workout example. First of all, the domain size $N = 353$, and its primitive root $\alpha = 3$. Alice and Bob select private keys: $A = 97$, and $B = 233$ respectively. Then, each of them computes a public key: Alice computes $X = 3^{97} \ mod \ 353 = 40$. Bob computes $Y = 3^{233} \ mod \ 353 = 248$. After that, they exchange public keys with each other and compute the secret keys in the following way:
Alice computes $K = (Y)^A \ mod \ 353 = 24897 \ \text{mod} \ 353 = 160$.
Bob computes $K = (X)^B \ mod \ 353 = 40233 \ mod \ 353 = 160$.

The goal of this research paper is to incorporate a signature scheme into my previously developed cryptosystem. To do that, this research paper is going to show a new crypto-intensive technique based on the Diffie-Hellman key exchange protocol, the concept of modular arithmetic, the floor function, the absolute value calculation, the square root, the quadratic quatotionet, and the quadratic residue. Moreover, three arithmetic operations are used in this cryptosystem: addition, multiplication, and division; In addition to that, authentication is done through signature generation and signature verification systems.

The encryption is accomplished by hashing the message twice: $H_1 = (m^2 \ mod \ K_c)$, $H_2 = \lfloor m^2 \div K_c \rfloor$. Signatur is given by a four-tuple (H_1, H_2, R_p, r_e). In the signature, the equivalent residue(r_e) is selected by satisfying the congruence relation of an expression $H_1(H_1 + G) \equiv H_1 * H_2 * R_p \ (mod \ K_c)$. A random padd($R_p$) is selected arbitrarily from a range of numbers, i.e., $\{1,2 \ldots \ldots N\}$ to justify the truthiness of the congruence relation. The signature is verified by checking the equality of the equation $r_e = H_1 * H_2 * R_p \ \text{mod} \ K_c$. If the left-hand side and right-hand side of the equation are eqaul, the verifier accepts the signature, and then opens the message using the expression $(D) = \left| \sqrt{H_2 * K_c + H_1} \right|$. The importance of this research in a cryptographic context is immense.

The subsequent roadmap for the article is laid out as follows: Section 2 contains a literature review; Section 3 presents the author's contribution; Section 4 provides discussion; Section 5 gives a conclusion; Section 6 gives acknowledgement; and the last section gives references as well as the author's biography.

https://doi.org/10.14299/ijser.2019.10.01

2 LITERATURE REVIEW

The Michael O. Rabin cryptosystem has a great theoretical significance in terms of cryptographic context. Normally, a cryptosystem is a combination of three algorithms: key generation, encryption, and decryption algorithm. As we know, the Rabin cryptosystem was the first asymmetric cryptosystem in public-key cryptography [9]. The Rabin signature scheme is one of the first digital signature schemes. Rabin's signature on a message (m) may consist of a single and a pair (m, s). However, if there is no solution of an equation $x^2 = m \bmod N$, the signature cannot be generated directly. To overcome this issue, many researchers proposed different ideas. To dive into the details, Let's discuss some preliminaries.

2.1 Preliminaries

Assuming that $N = p * q$ be a product of two odd primes p and q. Using the generalized Euclidean algorithm to compute the greatest common divisor between p and $q \in N$.

1. Initialize $r_0 = q$ and $r_1 = p$.
2. Compute the following sequence of equations:
   $r_0 = q_1 r_1 + r_2$, where q_1 is quotient.
   $r_1 = q_2 r_2 + r_3$,
   $r_{n-3} = q_{n-2} r_{n-2} + r_{n-1}$,
   $r_{n-2} = q_{n-1} r_{n-1} + r_n$, until there is a step for which
   $r_n = 0$, while $r_{n-1} \neq 0$.
3. The greatest common divisor is equal to r_{n-1}.

From which two integer numbers can be achieved after extending the theorem, and that is Bezout's coefficient $\lambda_1, \lambda_2 \in \mathbb{Z}$, such that $\lambda_1 p + \lambda_2 q = 1$, are efficiently computed. Thus, setting $\psi_1 = = \lambda_2 q$ and $\psi_2 = \lambda_1 p$, so that $\psi_1 + \psi_2 = 1$, it is easily verified that ψ_1 and ψ_2 satisfy the relations.

$$\begin{cases} \psi_1 \psi_2 = 0 \bmod N \\ {\psi_1}^2 = \psi_1 \bmod N \\ {\psi_2}^2 = \psi_2 \bmod N \end{cases}$$

and that $\psi_1 = 1 \bmod p$, $\psi_1 = 0 \bmod q$, and $\psi_2 = 0 \bmod p$, $\psi_2 = 1 \bmod q$. According to the Chinese Remainder Theorem (CRT), using ψ_1 and ψ_2 every element a in $\mathbb{Z}_N$ can be represented as $a = a_1\psi_1 + a_2\psi_2 \bmod N$, where $a_1 \in \mathbb{Z}_p$ and $a_2 \in \mathbb{Z}_q$ are calculated as $a_1 = a \bmod p$ and $a_2 = a \bmod q$. The four roots $x_1, x_2, x_3, x_4 \in \mathbb{Z}_N$ of $x^2 = C \bmod N$ represented as positive numbers, are obtained using the CRT from the roots u_1, $u_2 \in \mathbb{Z}_p$ and $v_1, v_2 \in \mathbb{Z}_q$ of the two equations $u_2 = C \bmod p$ and $v_2 = C \bmod q$, respectively. The roots u_1 and $u_2 = p - u_1$ have different parities; likewise, v_1 and $v_2 = \mathrm{q} - \mathrm{v}_1$. If p is congruent 3 modulo 4, the root u_1 can be computed in deterministic polynomialtime as $\pm C^{(p+1)/4} \bmod p$, $\pm C^{(q+1)/4} \bmod q$. However, u_1 can be computed in probabilistic polynomialtime using Tonelli's algorithm [10] once a quadratic non-residue modulo p is known (this computation is the probabilistic part of the algorithm), or using the probabilistic algorithm - Cantor-Zassenhaus algorithm [11, 12, 13] to factor the polynomial $u^2 - c$ modulo p. Using the previous notations, the four roots can be written as follows:

$$\begin{cases} \mathrm{x}_1 = \mathrm{u}_1\psi_1 + \mathrm{v}_1\psi_2 \bmod \mathrm{N} \\ \mathrm{x}_3 = \mathrm{u}_2\psi_1 + \mathrm{v}_1\psi_2 \bmod \mathrm{N} \\ \mathrm{x}_3 = \mathrm{u}_2\psi_1 + \mathrm{v}_1\psi_2 \bmod \mathrm{N} \\ \mathrm{x}_4 = \mathrm{u}_2\psi_1 + \mathrm{v}_2\psi_2 \bmod \mathrm{N} \end{cases}$$

Lemma 1: Let $N = p * q$ be a product of two prime numbers, and C be a quadratic residue modulo N. The four roots x_1, x_2, x_3, x_4 of the polynomial $x^2 - C$ are partitioned into two sets $X_1 = \{x_1, x_4\}$ and $X_2 = \{x_2, x_3\}$ such that roots in the same set have different parities, i.e., $x_1 = 1 + x_4 \bmod 2$ and $x_2 = 1 + x_3 \bmod 2$.

Proof. Since u_1 and v_1 have the same parity by assumption, x_1 and x_4 also have the same parity. The connection between x_1 and x_4 is shown by the following chain of equalities: $x_4 = u_2\psi_1 + v_2\psi_2 = (p - u_1)\psi_1 + (q - v_1)\psi_2 = -x_1 \bmod N = N - x_1$, because $p\psi_1 = 0 \bmod N$ and $q\psi_2 = 0 \bmod N$, and x_1 is less than N by assumption, thus $-x_1 \bmod N = N - x_1$ is positive and less than N. A similar chain connects x_2 and $x_3 = N - x_2$, because N is odd and thus x_1 and x_4 as well as x_2 and x_3 have different parities. Let's use those ideas to explore the Michael O. Rabin Signature Scheme and its subsequent varieties.

2.2 An illustration of Michael O. Rabin Signature

Firs of all, let's see an illustration of Rabin Signature scheme. *Sigining Algorithm:* The unique signature (S) is given by the $S = \left(\left(p^{q-2} H(m)^{\frac{q+1}{4}} \bmod q\right) p + \left(q^{p-2} H(m)^{\frac{p+1}{4}} \bmod p\right) q\right) \bmod \mathrm{N}$ and Verification is done by $H(m) = s^2 \bmod N$, where N is the composite number of $p * q$. The signature can be verified by everyone, as N is a public key. A hash function H is collision resistant if it is hard to find that hash with the same output. If H is a collision resistant hash function, that does not mean that no collision exists; simply, they are hard to find. Such as,

$$H(m)^{\frac{p-1}{2}} \bmod p = 1 \text{ and } H(m)^{\frac{q-1}{2}} \bmod q = 1.$$

The cryptographic hash function is any mathematical equation. Message(m) is being hashed (encrypted). The hash value 1 is generated by using the private keys p and q. The same hash value from different hashed inputs is so called collision resistant. The algorithm works in the following way: A workout example. let's create two prime number $p = 7$ and $q = 11$ using the prime formation $(4k + 3)$, whereas, $k = \{1,2,\ldots..n\}$. The public key is generated by $N = p * q = 77$. The Hashed message $H(m) = 20^2 \bmod 77 = 15$. The collision-resistant hash value will be $(15)^{\frac{7-1}{2}} \bmod 7 = 1$ and $15^{\frac{11-1}{2}} \bmod 11 = 1$ that is vulnerable to collision attacks, because a collision at-

https://doi.org/10.14299/ijser.2019.10.01

tack on a cryptographic hash tries to find two inputs producing the same hash value. The signature is given in the following way:

$S = ((7^{11-2}\ 15^{\frac{11+1}{4}}\ mod\ 11)7 + (11^{7-2}\ 15^{\frac{7+1}{4}}\ mod\ 7)\ 11)\ mod\ 77$
$= \big((8 * 9\ mod\ 11)7 + (2 * 11\ mod\ 7)11\big) mod\ 77$
$= (6 * 7 + 2 * 11)\ mod\ 77 = 64$. So, the signature is unique. And then signature verification is done in the following way: H (m) $= s^2$ mod 77 = 642 mod 77 = 15. Since H(m) = H(m), the signature is valid and accepted by the verifier. Now let's see a description of pairing signature algorithm.

key generation: In most presentations in modern cryptography, the algorithm is simplified by choosing b = 0, where b is actually the least prime (basement). The signer (S) chooses two prime numbers, p and q, respectively and computes the product of them $N = p * q$, whereas N is declared as a public key.

Signature generation: Signer S picks random padding U to sign a message m and calculates $H\ (m) * U\ mod\ N$. Signer(S) then solves the equation $X(X + b) = H\ (m) * U mod\ N$. where b is the basement (least prime). If there is no solution, S picks up a new pad U and tries again. Otherwise, the signature on m is (U, x).

Signatue Verification: Given a message m and a signature (U, x), the verifier (v) calculates the equality of $X(X + b)\ mod\ N$ and $H(m) * U\ mod\ N$, where $X = H(X)$. If equality is found, the signature is accepted. For example, assume that an entity A wants to send secret information $(X = 20)$ to another entity B using a valid signature. It first hashes the secret by $m^2\ mod\ N = 20^2\ mod\ 77 = 15$. Where N is a composite number of two secret private keys, moduli $p = 7$, moduli $q = 11$, both prime are Blum prime (4k+3). Public key or modulus $N = p * q = 7 * 11 = 77$. The Hashed value of 15 will be used to generate signatures.

Signing process: Signer (S) chooses the number U probabilistically and see that the value of a random oracle modulo N matches any quadratic residue modulo N that is $X\ (X + b)\ mod\ N = m * U\ modulo\ N$. This process continues until both sides of the equation match the hash.

$X(X\ +\ b)\ mod\ N$	$m * U\ mod\ N$
$= 15\ (15 + 2)\ mod\ 77$	$=\ (15 *\ 17)\ mod\ 77$
$=\ 24$	$= 24$

The equation is solvable, which is why the signature on message(m) is the pair (17, 15). So, it's clear that Rabin's signature on a message m may consist of a single and a pair (m, S). However, if there is $x^2 = m\ mod\ N$ has no solution, this signature cannot be directly generated. To overcome this obstruction, a random pad U was proposed by J. Pieprzyk et.al. [14], and attempts are repeated until $x^2 = m * U\ mod\ N$ is solvable, and thus the signature is the triple (m, U, S). A verifier compares $m * U\ mod\ N$ with S^2 and accepts the signature as valid when these two numbers are equal. Let's see other researchers's findings in this area. Hugh Cowie William [15] develop a modification of the Rabin system that allows the cryptographer to definitively decide which of the four-square roots the original message is. The Rabin-Williams signature scheme relies on finding the difficulties in the square root. It avoids the fraud vulnerabilities. It does not offer multiple signatures in one document. However, scheme requires the use of two primes congruent to 3 and 7 modulo 8, respectively. Additionally, in the Rabin-Williams scheme, a message cannot be signed twice in two different ways. The factorization otherwise of N might get exposed, otherwise.

Michele Elia, et al. [16] presented a modification of the H. C. William scheme based on the computation of a Jacobi symbol, where a deterministic pad is used for calculating non-Blum prime and Blum prime when m is QNR, as follows:

$$f_1 = \frac{m_1}{2}\left[1 - \left(\frac{m_1}{p}\right)\right] + \frac{1}{2}\left[1 + \left(\frac{m_1}{p}\right)\right]$$
$$f_2 = \frac{m_2}{2}\left[1 - \left(\frac{m_2}{q}\right)\right] + \frac{1}{2}\left[1 + \left(\frac{m_2}{q}\right)\right]$$
$$m = (m_1\psi_1 + m_2\psi_2)\ mod\ n$$

$x^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = (f_1 m_1\psi_1 + f_2 m_2\psi_2)$ $mod\ N$, where $f_1 m_1$ and $f_2 m_2$ is a quadratic residue $modulo\ p$ and $modulo\ q$ respectively, Since $\left(\frac{m_1}{p}\right) = \left(\frac{f_1}{p}\right), \left(\frac{m_2}{q}\right) = \left(\frac{f_2}{q}\right)$ so that $\left(\frac{m_1 f_1}{p}\right) = \left(\frac{m_1}{p}\right)\left(\frac{f_1}{p}\right) = 1$ and $\left(\frac{m_2 f_2}{q}\right) = \left(\frac{m_2}{q}\right)\left(\frac{f_2}{q}\right) = 1$
$u = R^2\ [f_1\psi_1 + f_2\psi_2]$. *Signed message*: (m, u, s), *Verification:* Signer verifies the equality of the equation $x^2 = \text{m} * \text{u mod N}$. If $L.H.S = R.H.S$, the signature is considered to be valid for message(m). This is deterministically true as x^2 pre-calculated, but probabilistically, there is no such x value for which the $x^2 = \text{m} * \text{u mod N}$ is true.

Evgeny Sidorov et al. [17] described a bug in the implementation of Rabin-Williams digital signature in the crypto++ framework, which is a popular cryptographic framework. The bug is in the misuse of blinding techniques that are aimed at preventing timing attacks on the digital signature system implementation. To fix the bugdoors, one need to ensure that the value used for blinding is a quadratic residue modulo p and q. This condition guarantees that the blinding value will be removed at the unblinding step and won't affect the result of the signing procedure. Although, authors aimed at improving the security of the Rabin-Williams signature. They eventually made the system completely insecure, as admitted by authors themselves. The Rabin-Williams signatures became more efficient with the state-of-the-art modular–root signature system which was far beyond the simple signature system introduced by Daniel J. Bernstein [18]. Michele Elia et al. [19] described a variant aimed at countering Rabin's signature vulnerability. The detail explanation of the procedure is as follows:

Signed Message: $(m, U * R^2\ mod\ N, S * R^3\ mod\ N, R^4\ mod\ N)$, so the signature is a fourtuple where U is the padding factor and R is a random number selection, Here S is the x's value

https://doi.org/10.14299/ijser.2019.10.01

for which the equation $x^2 = m * U \ mod \ N$ is true. It is clearly seen that x and U are both unknown numbers that have to be chosen by entity A in order to generate a signature.

Verification process: Compute $(S * R)^2 \text{mod N}$ and $m * U * R^2 * R^4 \ mod \ N$; the signature is valid if and only if the aforesaid two numbers are equal. Let's see an example, assuming preprocessed values for $m^{/} = 15, U * R^2 = 25 * 3^2 \ mod \ 77 = 71, S * R^2 = 12 * 3^2 = 108 \ mod \ 77 = 48$ and $3^4 \ mod \ 77 = 4$. So, the four-tuple signature is $(15, 71, 48, and \ 4)$. The process of verification can be described by two-step: in 1st step, computing $(12 * 3^3)^2 \ mod \ 77 = (12^2 * 3^6) \ mod \ 77 = 25$, and in 2nd step, computing $(15 * 25 * 3^2 * 3^4) \ mod \ 77 = 25$. Since, counter forgery four-tuple signature (15, 71, 48, and 41) verification is successful, the signature is valid and accepted.

Jaweria Usmani et al. [20] proposed a secure gateway discovery protocol using the Rabin Signature Scheme in MANET that ensures confidentiality in heterogeneous environments. The registration process was included to remove the malicious nodes. This protocol removes the threat of anti-confidentiality, anti-authentication, and anti-duplication. The efficiency of this protocol is shown through the AVISPA tool. Chaoyang Li et al. [21] proposed an efficient ID-based signature scheme based on Rabin's cryptosystem by using the forking lemma theorem. This scheme has a lower exponential operation. It is secure against existential forgery under adaptively chosen identity and message attacks in the random oracle model. Daniel Bleichenbacher [22] presents a method to compress Rabin signature. The rabin signatures and compressed signatures are equally difficult to forge. Compression requires a continued fraction expansion and takes time $0(log(n)_2)$. Decompression requires two multiplications and an inverse over $\mathbb{Z}/_n\mathbb{Z}$, a square root of $\mathbb{Z}$ which requires time $0(log(n)_2)$.

Based on mathematical analysis of other people's findings in various contexts of cryptosystems and signature schemes, my research is focusing on attaching a signature scheme to a cryptosystem using the mathematical ideas derived from a literature review.

A. AIMS AND OBJECTIVES

The goal of the research is to construct a signature scheme and connect it to my previously built cryptosystem. And therefore, the following research questions are formulated from the research objectives to conduct this research:

RESEARCH QUESTIONS

1. What mathematical function do I need for a signature scheme?
2. How do I incorporate a signature scheme into a cryptosystem?

3 AUTHOR'S CONTRIBUTION

3.1 Key generation algorithm: $\text{K} = (Y_b)^{xa} \ mod \ N$ $= (\alpha^{xb} mod \ N)^{Xa} mod \ N$ $= (\alpha^{xb})^{Xa} mod \ N$ $= \alpha^{xb \, . \, Xa} mod \ N$ $= (\alpha^{Xa})^{xb} \ mod \ N$ $= (\alpha^{Xa} mod \ N)^{Xb} mod \ N$ $= (Y_a)^{xb} mod \ N$	Diffie-Hellman Key Exchange protocol
3.2 Current key $(K_c) = P_{sk} + K$, whereas P_{sk} is a pre-negotiated symmetric key, and K is an exchange key.	Security Key
3.3 Encryption technique: $\text{H}_1 = \text{m}^2 \text{ mod } K_c$ $\text{H}_2 = \lfloor \text{m}^2 \div K_c \rfloor$ $\text{C} = (\text{H}_1, \text{H}_2)$, where C = Ciphertext. H = Hash messaege	Message Hiding
3.4 Signature generation: Signature: $(\text{H}_1, \text{H}_2, R_p, \text{r}_\text{e})$ $\text{H}_1(\text{H}_1 + \text{G}) \equiv \text{H}_1 * \text{H}_2 * \text{R}_\text{p} \ (\text{mod } K_c)$ where r_e is an equivalent residue, R_p is a Random Pad.	Message Authentication
3.5 Signature verification: $\text{r}_\text{e} = \text{H}_1 * \text{H}_2 * \text{R}_\text{p} \ \text{ mod } K_c$	Message Validation
3.6 Decryption technique: $D = \left\lfloor \sqrt{H_2 * K_c + H_1} \right\rfloor$	Opening message

4 DISCUSSIONS

Let's say that an entity A exchanges information with another entity B. Both entities A and B should have some privacy. Both entities A and B generate a shared secret key using the aforementioned key exchange protocol, and then both add an additional pre-negotiated secret key to the newly generated key, i.e., $K_c = P_{sk} + K$. Alice encrypts the secret information with a secret key so that an unauthorized entity cannot guess and reveal the real information. When the key exchange is complete, Alice hashes the message (H_m) in two ways: $H_1 = m^2 \ mod \ K_c$ and $H_2 = \lfloor m^2 \div K_c \rfloor$ to encrypt the message. Next, she picks a random padd $(R_p) = \{1, 2 \ldots . n\}$ to sign a message (m) and calculates $H_m * R_p \text{ mod } K_c \Longrightarrow H_1 * H_2 * R_p \text{ mod } K_c$. She then solves the congruent relation of the equation $H_1(H_1 + G) \equiv H_1 * H_2 * R_p \ (modulo \ K_c)$. If there is no solution for the first picking random padd, she picks up another random padd (R_p) until the congruent relation exists. If equality is found, she creates a four-tuple signature (H_1, H_2, R_p, r_e). Note that H_1 is the quadratic residue, H_2 is the floor value of the quadratic quotient, and $R_p = \{1,2, \ldots \ldots \ldots n\}$ is a random padd, G is the generator, r_e is an equivalent residuum. After

https://doi.org/10.14299/ijser.2019.10.01

that, Alice sends only a four-tuple signature (H_1, H_2, R_p, r_e) for a given message (m) to Bob. Afterwards, in the signature verification process, Bob verifies the signature depending on the equality of the equation $r_e = (H_1 * H_2 * R_p)$ modulo K_c. Later, Bob opens the message with the expression $(|\sqrt{H_2 * K_c + H_1}|)$ if and only if the equation $r_e = (H_1 * H_2 * R_p)$ modulo K_c holds true; otherwise, rejects. Let's see an example. Suppose, Alice wants send a message ($A = 65$ ASCII Value) to Bob using a valid signature. To do that, first of all, both Alice and Bob generate a shared secret key using the Diffie-Hellman key exchange protocol in the following way:

Pre-negotiated secret key (p_{sk}): {1 … … n}					
Alice		Evesdroper		Bob	
known	un-known	known	unknown	Known	un-known
N=113		✓		✓	
$G = 5$		✓		✓	
P = 7	Q = 11		P = 7 Q = 11	Q = 11	P = 7
$A = 5^7(113) = 42$		Dynamic		$B = 5^{11}(113) = 34$	
$A = 34^7(113) = 40 = k_a$		Swapping		$B = 42^{11}(113) = 40 = k_b$	
$k_c = k_a + p_{sk} = 40 + 17 = 57$				$k_c = k_b + p_{sk} = 40 + 17 = 57$	

Current key (k_c) = exchange key + pre-negotiated key. Alice and Bob obtain a new key by mixing the exchange with the default key. The default key protects against man-in-the-middle attacks because they both exchange their keys publicly. Although the eavesdropper may obtain the exchange key, he does not have access to the previously discussed key. Alice locks the written message using the current key (k_c). She then signs the encrypted message and sends it to Bob.

Message encryption process:
Alice hashes the message $A = 65$ (ASCII Value) in two ways:
Hash message $(H_1) = (65)^2 \, mod \, 57 = 7$
Hash message $(H_2) = \lfloor (65)^2 \div 57 \rfloor = 74$
Cyphertext $(C) = H(m) = (H_1, H_2)$.

Signature generation process: Alice picks one random padd (R_p) arbitaryliy. Note that the value of R_p can be any number, i.e.,$R_p = \{1,2, \dots \dots n\}$. but given condition says that we have to choose such a number for which the value of $H_1(H_1 + G)$ mod K_c and $H_1 * H_2 * R_p$ mod K_c must be equal. i.e., $H_1(H_1 + G) \equiv H_1 * H_2 * R_p \, (mod \, K_c)$. For instance, for the random number 51, the congruence relation holds true.

$\Rightarrow 7(7 + 5) \equiv 7 * 74 * 51 \, (mod \, 57) \Rightarrow 27 \equiv 27 \, (modulo \, 57)$. Let it say equivalent residue $r_e = 27$, Hence, she gernerates a four-tuple signature (7, 74, 51, and 27) on message $A = 65$.

Signature verification process: Bob verifies Alice's signature, relying on the equality of the following equation:
$r_e = H_1 * H_2 * R_p \bmod K_c \Rightarrow r_e = 7 * 74 * 51 \bmod 57 \Rightarrow$
$r_e = 27 \Rightarrow 27 = 27$, verified.

Message opening process:
Since the signature is valid, Bob unlocks the secret message by adding a square root to the expression $(H_2 * K_c + H_1)$ and accepting only the absolute value as the desired plaintext.
Decryption: $D = |\sqrt{H_2 * k_c + H_1}| = |\sqrt{74 * 57 + 7}| = |\sqrt{4225}| = 65 = A \, (reveal)$.

.

4.1 COMPARISON

Advantages of the Michael O. Rabin Signature: The signature actually contains several interesting features: The signature is possible using every pair of primes. Different signatures on the same document are different. The verification needs only two multiplications, and therefore it is fast enough to be used in the authentication protocol.

Disadvantages of Michael O. Rabin Signature: It is vulnerable to forgery attacks. It is relatively easy to compute $S^2 \, mod \, N$, choose any message $m^/$ and compute the multiplicative inverse of the $m^/$(hash value of m); compute $U^/ = S^2 * m^{/-1} \bmod N$ and forge the signature as ($m^{/-1}$, $U^/$, S) without knowing the factorization of N.

Advantages of MSH Biswas Crypto-intensive technique: The signature (H_1, H_2, R_p, r_e) is generated by two-step hashed message, one random padd, and an equivalent residuum. It is sequre against man-in-the-middle and forgery attack. It does not rquire computing four roots. It requires less time complexity compared to the Michael O. Rabin public key signature scheme. The MSH Biswas crypto-intensive technique is efficient for solving four-to-one mapping signatures. It can efficiently identify each ciphertext separately because modular arithmetic sometimes generates the same ciphertext from different plaintexts. The proposed signature scheme can verify the sender and validate the message through a signature verification system. In this system, both authentication and integrity components have been successfully deployed.

5 CONCLUSIONS

To conclude the investigation into the Rabin cryptosystems and signature schemes, the Rabin cryptosystems and Rabin signature schemes were analyzed. And then, the purpose of the study was completed by incorporating a signature scheme into my previously developed cryptosystem. The correctness

https://doi.org/10.14299/ijser.2019.10.01

of the MSH Biswas crypto-intensive was finalized based on the mathematical induction method. The ambiguities of Rabin cryptosystems and the vulnerability of Rabin signature schemes were finalized based on a literature review, findings, and a focus group discussion. After conducting this research, it was concluded that Rabin signature schemes are vulnerable to a forgery attack. The Diffie-Hellman key exchange protocol cannot authenticate the participants. But, the proposed crypto-enabled technique ensures security by combining an exchange key with a pre-negotiated key that is unknown to the adversary. The objective of this research has been successfully achieved.

A. RECOMMENDATION

Based on the conclusion, some recommendations are prepared for researchers: I would like to leave my encryption scheme as a challenge for future readers and welcome cryptographic researchers to make a concrete (single) ciphertext that can uniquely identify each quadratic residue generated from different inputs.

B. LIMITATION

This is a very simple cryptographic concept. This research work has been done for academic purposes only. So, it may not be suitable for professional work.

6 ACKNOWLEDGEMENTS

I am very grateful to my family members who provided financial support to conduct this study. Without their financial support, I could not conduct this research, and its publication could not even take place. I am grateful to all of my well-wishers and friends. I thank Dr. Md. Mostafijur Rahman and Md. Maruf Hassan for their inspirational advice. This article is part of the thesis and research activities of Daffodil International University for the academic curriculum fulfillment of an MSc. in Software Engineering & Cybersecurity.

REFERENCES

[1] Michael O Rabin. Probabilistic algorithms algorithms and complex ity: New directions and recent results, *ACADEMIC PRESS, INC. New York San Francisco*, December 1976, pp. 21-40

[2] Michael O Rabin, "Digitized signatures and public key functions as intractable as factorization". *technical report MIT-LCS-TR-212*, MIT laboratory for computer science, 1979.

[3] Johannes A Buchmann, Stephan D¨ullmann, and Hugh C Williams. "On the complexity and efficiency of a new key exchange system". In: *Advances in Cryptology—EUROCRYPT'89: Workshop on the Theory and Application of Cryptographic Techniques Houthalen, Belgium, April 10–13, 1989 Proceedings 8*, pages 597–616. Springer, 1990.

[4] Joseph H Silverman, Jill Pipher, and Jeffrey Hoffstein. "An introduce tion to mathematical cryptography". 1, Springer, New York, 2008.

[5] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. "Handbook of Ap plied Cryptography", CRC Press, Boca Raton, 1997.

[6] Public-Key Cryptography. For a comprehensive technical discussion of public-key cryptography and cryptographic algorithms, see Bruce schneier, applied cryptography, Wiley, 1996.

[7] PaulC.Kocher, "Timing Attacks on Implementations of Diffie-Hell man, RSA, DSS, and other systems ". Cryptography Research, Inc, In: *Advances in Cryptology - CRYPT0 '96: 16th Annual Interntional Cryptology Conference Santa Barbara*, california, usa,1996 proceedings 16, pages 104–113. Springer, 1996.

[8] Bert Den Boer. "Diffie-hellman is as strong as discrete log for certain primes". In: *Conference on the Theory and Application of Cryptography*, pages 530–539. Springer, 1988.

[9] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. "Mi chael.O. Rabin cryptosystem". In: *Handbook of applied cryptography*. CRC press, 2018.

[10] Eric Bach and Jeffrey Outlaw Shallit. In: *Algorithmic number theory: Efficient algorithms*, volume 1. MIT press, 1996.

[11] David G Cantor and Hans Zassenhaus. "A new algorithm for fac toring poly-nomials over finite fields". In: *Mathematics of Computa tion*, Vol. 36, N. 154, pages 587–592, 1981.

[12] Michele Elia and Davide Schipani. "Improvements on the cantor-zassenhaus factorization algorithm". In: *Mathematica Bohemica*, 140(3):271–290, 2015.

[13] Joachim Von Zur Gathen and J¨urgen Gerhard. "Modern computer algebra". *Cambridge university press*, 2003.

[14] J. Pieprzyk, T. Hardjono, J. Seberry, Fundamentals of Computer Secu rity, Springer, New York, 2003.

[15] H.C. Williams, A modification of the RSA public-key encryption procedure, IEEE Trans. on Inform. Th., IT-26(6), November 1980, pp.726-729.

[16] Michele Elia, Davide *Schipani.* "On the Rabin signature". In: *Journal of Discrete Mathematical Sciences and Cryptography*, 16(6). Pages 367–378, 2013.

[17] Evgeny Sidorov. "Breaking the Rabin-Williams digital signature system Implementation in crypto++ library" In: *Journal of cryptology*, ePrint Archive, 2015.

[18] Daniel J. Bernstein. "RSA and Rabin-Williams signatures: the state of the art". In: *EUROCRYPT, Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Ad vances in cryptology,* volume 6, Pages 70-87, 2008.

[19] Michele Elia, Matteo Piva, and Davide Schipani. "The Rabin cryptosy stem revisited". In: *Applicable Algebra in Engineering, Communication and Computing, 26, pages 251-275*, 2015.

[20] Usmani Jaweria and Jay Prakash. "A Secure Gateway Discovery Protocol Using Rabin Signature Scheme in MANET". In: *Interna tional Journal on Communications Antenna and Propagation*, 7(5):439, 2017. DOI: 10.15866/irecap. v7i5.12581

[21] Chaoyang Li1, Xiangjun Xin2, and Xiaolin Hua." Efficient ID-based Rabin Signature without Pairings". In: *International Journal of Multi media and Ubiquitous Engineering*, 12(3), pages 75-80, 2017. doi: 10.14257/jimue.2017.12.3.08

[22] Daniel Bleichenbacher. "Compressing Rabin Signatures". In: *Cryp tographers' Track at the RSA Conference*.pages 126-128. Springer 2004.

Author Biography

Name: Md. Shamim Hossain Biswas
MSc in Software Engineering (Cybersecurity), Daffodil International University
BSc in Computer Science & Engineering, Stamford University Bangladesh
E-mails: shamim.ak.pico@gmail.com, shamim44-165@diu.edu.bd
ORCID: 0000-0002-4595-1470